ABSTRACT

A method is disclosed comprising placing a first device in an enclosure, placing a second device in the enclosure, sealing the enclosure, and after sealing the enclosure, causing the first device to exchange a key with the second device. After the key exchange, the first and second devices can be taken out of the enclosure and can use the key to communicate with each other securely and in an authenticated manner. The devices may be electronic devices or optical devices. The enclosure prevents electromagnetic radiation of a certain bandwidth from escaping and thus prevents an adversarial device from eavesdropping on communication between the first and second devices. The enclosure may include a filtering material such as a metal net. The enclosure may be, for example, a plastic bag or a glass container. The user may prepare two devices for a communication, such as a key exchange, by setting the two devices in a transfer mode, which may start the key exchange by a timer in one of the devices, then place them in the container, and seal the container. When the devices have finished the communication such as a key exchange, this fact may be signaled by sound or in some other manner by the devices. The container may have a separate compartment for each device and the compartments may be separated by a separation device such as a door comprised of filtering material. When both compartments are properly closed, the users may open the door allowing the two devices to discover each other and communicate or exchange encryption keys. The container may include a Bluetooth or other transmitter, connected to the outside world by means of cord device. The cord device may plug into a device outside of the container with which a key exchange is desired. A portable device is also disclosed in the form of for example, a floppy disc or a PCMCIA card.